TEAM YOKOTA OPSEC AWARENESS Quarterly Newsletter 2016

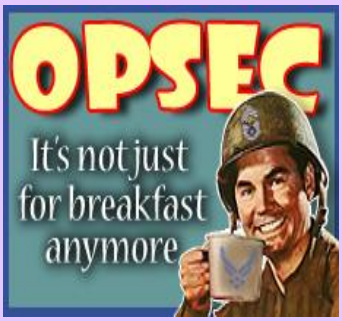
How does the adversary gather critical information???

- Communication Intercept
- Conversations in public areas
- Using cell phones for business
- Web pages
- E-mail
- Social Networking
- Social Engineering
- Internet
- Elicitation
- Espionage

Do's and Don'ts for Unclassified Information

DO NOT:

- Post sensitive information on social networking sites, such as Facebook, Twitter, YouTube, etc.
- Post sensitive information on public websites
- Place sensitive information in trash cans or recycle bins
- Leave sensitive information in vacated offices
- Leave sensitive information unattended
- Allow access to those individuals without a "need to know"
- Place sensitive information on shared drives, unless password protected



DO:

- Encrypt e-mail when sending sensitive information
- Review information for sensitivity prior to posting on social networking sites
- Review information for sensitivity prior to posting on all websites
- Ensure only unclassified non-sensitive information is discarded in trash and recycle bins
- Conduct an annual clean-out each year
- Ensure you have enough supplies (burn/shred bags) on hand to discard of sensitive information
- Look behind desk drawers and under desks for information that may have fallen
- Create passwords that can not be duplicated

374 AW OPSEC Team
Major Booe – 225-7811
Capt Howell – 225-7811
Mr. Renteria – 225 8361

Interested in additional OPSEC training?

Please visit: www.iad.gov